

Local implementation of nonlocal operations with block forms

Ning Bo Zhao*, An Min Wang†

Quantum Theory Group, Department of Modern Physics

University of Science and Technology of China, Hefei 230026, People Republic of China

We investigate the local implementation of nonlocal operations with the block matrix form, and propose a protocol for any diagonal or offdiagonal block operation. This method can be directly generalized to the two-party multiqubit case and the multiparty case. Especially, in the multiparty cases, any diagonal block operation can be locally implemented using the same resources as the multiparty control-U operation discussed in Ref. [1]. Although in the bipartite case, this kind of operations can be transformed to control-U operation using local operations, these transformations are impossible in the multiparty cases. We also compare the local implementation of nonlocal block operations with the remote implementation of local operations [2], and point out a relation between them.

PACS numbers: 03.67.Lx

I. INTRODUCTION

Nonlocal operations are critical in distributed quantum computation. Sometimes, a collective operation needs to be implemented on the qubits at distant nodes. Generally, such an operation can not be implemented directly. However, it is possible to be implemented locally, i.e., it can be implemented using local operations and classical communications (LOCC), shared entanglement and some auxiliary qubits. Obviously straightforward method to implement such a nonlocal operation is using quantum state teleportations [3], i.e., teleporting all of the qubits to one node, performing the operation at this node and teleporting these qubits back.

In the bipartite case, it requires two rounds of state teleportation and one local collective operation to implement a nonlocal operation using the above method. So this process consumes two ebits (shared entanglement resources) and four cbits (classical communications). These resources are necessary for some operations such as the SWAP operation [1, 4]. However, there are operations that can be locally implemented using less resources [1, 4]. For the CNOT operation, the necessary and sufficient resources are one ebit plus two cbits — one cbit for each direction. These resources are also sufficient for general control-U operations. Ref. [1] presented a protocol to locally implement the CNOT operation just using these resources. This protocol has been experimentally demonstrated in Ref. [5]. Ref. [1] also pointed out that a similar protocol — replacing one CNOT operation by the control-U operation — can be used for general control-U operation.

In Sec. II, we propose a similar protocol of local implementation of nonlocal operations with diagonal or offdiagonal block forms, using the same resources. This protocol is free of the specific content of the blocks, so it is available even if these blocks are unknown. This protocol is also independent of the dimension of the blocks, so it can also be used in the case if there are multiqbuts at the node where the operation is actually implemented. We compare the local implementation of nonlocal block operations with the remote implementation of local operations in Sec. III. We generalize the protocol to the multiqubit cases in Sec. III and to the multiparty cases in Sec. IV. In Sec. V, we summarize our results.

Recently, the problems of constructing a nonlocal operation or simulating it by other operations are discussed [6, 7, 8, 9]. We do not discuss this problem in this paper. The problem discussed in this paper is how to locally implement a nonlocal operation using LOCC and shared entanglement resources if the device of the operation has been constructed in one node.

II. NONLOCAL BLOCK OPERATIONS ON TWO QUBITS

Consider these nonlocal diagonal block operations

$$U = \begin{pmatrix} u_0 & 0 \\ 0 & u_1 \end{pmatrix}, \quad (1)$$

* nbzhao@mail.ustc.edu.cn

† anmwang@ustc.edu.cn

where u_0 and u_1 are 2×2 unitary matrices. Alice and Bob need to implement such an operation on their qubits A and B , where qubit A belongs to Alice and qubit B belongs to Bob. Bob has the device to implement this operation. U in Eq. 1 can be expressed as

$$U^{A,B} = \sum_{i=0}^1 |i\rangle_A \langle i| \otimes u_i^B. \quad (2)$$

Let us propose the following protocol in order to locally implement such an operation on the qubits A and B .

In general, the jointed initial state of the qubits A and B can be expressed as

$$|\Psi_0\rangle_{AB} = \alpha_0|0\rangle_A |\xi_0\rangle_B + \alpha_1|1\rangle_A |\xi_1\rangle_B, \quad (3)$$

where $|\xi_0\rangle$ and $|\xi_1\rangle$ are arbitrary state and need not be orthogonal.

They share a maximally entangled pair A_1B_1 in the state

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (4)$$

where qubit A_1 belongs to Alice and qubit B_1 belongs to Bob.

step 1 Alice performs a CNOT operation on her qubits A and A_1 , using the qubit A as the control. After this, the state of A, B, A_1, B_1 becomes

$$\begin{aligned} & CNOT^{A,A_1} |\Psi_0\rangle_{AB} \otimes |\Phi\rangle_{A_1B_1} \\ &= CNOT^{A,A_1} \sum_i \alpha_i |i\rangle_A |\xi_i\rangle_B \frac{1}{\sqrt{2}} \sum_j |jj\rangle_{A_1B_1} \\ &= \frac{1}{\sqrt{2}} \sum_{ij} \alpha_i |i\rangle_A |\xi_i\rangle_B |i \oplus j\rangle_{A_1} |j\rangle_{B_1}, \end{aligned} \quad (5)$$

where “ \oplus ” denotes the addition module 2.

Then she measures the qubit A_1 in computational basis $|a\rangle\langle a|$, ($a = 0, 1$), and tell the result a to Bob via a classical communication channel. The state of A, B, B_1 becomes

$$\begin{aligned} & \sum_{ij} \alpha_i |i\rangle_A |\xi_i\rangle_B |j\rangle_{B_1} \delta_{a,i \oplus j} \\ &= \sum_{ij} \alpha_i |i\rangle_A |\xi_i\rangle_B |j\rangle_{B_1} \delta_{j,i \oplus a} \\ &= \sum_i \alpha_i |i\rangle_A |\xi_i\rangle_B |i \oplus a\rangle_{B_1}. \end{aligned} \quad (6)$$

step 2 If the result $a = 0$ Bob does nothing, if $a = 1$ Bob performs the operation X on B_1 , where

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (7)$$

is the first Pauli matrix. Because $X|i\rangle = |i \oplus 1\rangle$, ($i = 0, 1$), the state of A, B, B_1 becomes

$$\sum_i \alpha_i |i\rangle_A |\xi_i\rangle_B |i\rangle_{B_1}. \quad (8)$$

step 3 Bob performs the two-qubit operation U on his qubits B_1 and B . The state of A, B, B_1 becomes

$$\begin{aligned} & U^{B_1,B} \sum_i \alpha_i |i\rangle_A |\xi_i\rangle_B |i\rangle_{B_1} \\ &= \sum_i \alpha_i |i\rangle_A (u_i |\xi_i\rangle)_B |i\rangle_{B_1}. \end{aligned} \quad (9)$$

step 4 Bob performs the operation H on B_1 , where

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (10)$$

is the Hadamard operation. Because $H|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^i|1\rangle)$, the state of A, B, B_1 becomes

$$\begin{aligned} & \sum_i \alpha_i |i\rangle_A (u_i |\xi_i\rangle)_B \frac{1}{\sqrt{2}}(|0\rangle + (-1)^i|1\rangle)_{B_1}. \\ &= \frac{1}{\sqrt{2}} [|0\rangle_{B_1} \sum_i \alpha_i |i\rangle_A (u_i |\xi_i\rangle)_B + |1\rangle_{B_1} \sum_i (-1)^i \alpha_i |i\rangle_A (u_i |\xi_i\rangle)_B]. \end{aligned} \quad (11)$$

Bob measures B_1 in the computational basis $|b\rangle\langle b|$, $b = 0, 1$, and tell the result b to Alice via a classical communication channel. The state of A, B becomes

$$\sum_i (-1)^{ib} \alpha_i |i\rangle_A (u_i |\xi_i\rangle)_B. \quad (12)$$

step 5 If $b = 0$ Alice does nothing, if $b = 1$ Alice performs the operation Z on A , where

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (13)$$

is the third Pauli matrix. Because $Z|i\rangle = (-1)^i|i\rangle$, the state of A, B becomes

$$\sum_i \alpha_i |i\rangle_A (u_i |\xi_i\rangle)_B = U^{A,B} |\Psi_0\rangle_{AB}. \quad (14)$$

Thus, after these five steps, the diagonal block operation U are determinately implemented on A, B using 1 ebit and 2 cbits.

This protocol can be expressed as Fig. 1. It can be found that the protocol is the same as the protocol for the

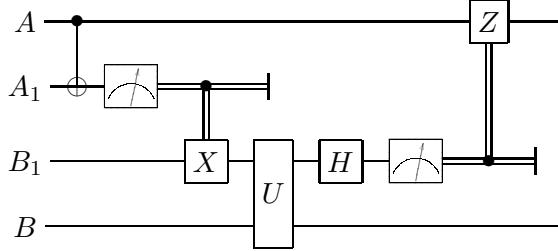


FIG. 1: Quantum circuit of the protocol for diagonal block operation, A_1 and B_1 is a maximally entangled pair in the state defined by Eq. 4.

CNOT operation or the control-U operations discussed in Ref. [1]. We have just proved that the same procedure can also be used for any diagonal block operation. This result is nontrivial for the following reasons.

Because the diagonal block operation

$$U = (I \otimes u_0)(|0\rangle\langle 0| \otimes I + |0\rangle\langle 0| \otimes u_0^\dagger u_1), \quad (15)$$

where I is the identity operation, so if U is completely known, it can also be implemented by performing a control-U operation $|0\rangle\langle 0| \otimes I + |0\rangle\langle 0| \otimes u_0^\dagger u_1$ and a single qubit operation u_0 . The control-U operation can be implemented using the protocol in Ref. [1]. However, if using this method, Bob must construct two new devices to implement these two operations. These accessory devices need consume more local resources and may bring a loss of accuracy. So if Bob already have the device of U , it is more economical and more accurate to directly use our protocol.

Furthermore, if Bob has the device of a diagonal block operation, but they do not know the detail of it, then they can not use other operations to simulate it. However, our protocol is still a choice for them, even in this case.

Investigating the proof of the protocol, it can be found that the protocol is independent on the dimension of the blocks. So if the blocks in Eq.(1) are $2^N \times 2^N$ unitary matrices, i.e., the diagonal block operation operates on $N + 1$

qubits — the first qubit belongs to Alice and the others belong to Bob, they can also locally implement this operation using the same protocol, just replacing the two-qubit operation by the $(N + 1)$ -qubit operation and replacing the qubit B by these N qubits correspondingly.

Consider an offdiagonal block operation, i.e., the operation can be expressed as

$$U^{A,B} = \sum_{i=0}^1 |i\oplus 1\rangle\langle i| \otimes u_i, \quad (16)$$

where u_i s are unitary matrices. They can locally implement such an operation using the same protocol, except that Alice need first perform an X operation on A in step 5. This accessory operation is a local operation at Alice's place, so it is commutable with Bob's local operations in step 2-4. Thus, Alice can perform this operation at anytime after step 1 and before step 5. The protocol for offdiagonal block operations can be expressed as Fig. 2. The validity of it can be proved similarly.

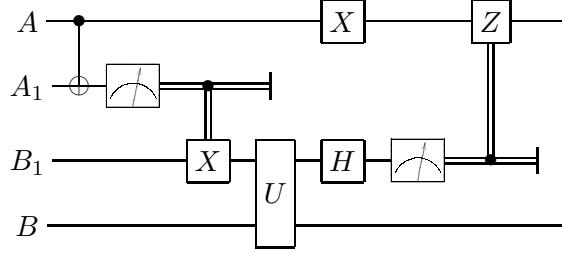


FIG. 2: Quantum circuit of the protocol for offdiagonal block operation, A_1 and B_1 is a maximally entangled pair in the state defined by Eq. 4.

III. BIPARTITE MULTIQUBIT

Consider the diagonal block operation in Eq. (1). If $u_0 = c_0 I$ and $u_1 = c_1 I$, then $U = (c_0|0\rangle\langle 0| + c_1|1\rangle\langle 1|) \otimes I$. Thus, U is actually a one-qubit diagonal operation, and the protocol in Sec. II is actually a protocol to remotely implement a diagonal operation from Bob to Alice. In fact, it is just the HPV protocol proposed in Ref. [10]. The only difference between the one-qubit diagonal operations and the two-qubit diagonal block operations is that the arbitrary coefficients are replaced by arbitrary unitary matrices, and the only difference between these two protocols is that the one-qubit diagonal operation is replaced by the two-qubit diagonal block operation. In general, intuitively, if there is a protocol for the remote implementation of “any” operation that can be expressed as

$$U^A = \sum_i c_i K_i, \quad (17)$$

where K_i s are certain matrices which can be regarded as the characteristic of the restricted set of the protocol, and c_i s are arbitrary coefficients, then the protocol may also be used to locally implement “any” block operation that can be expressed as

$$U^{A,B} = \sum_i K_i \otimes u_i, \quad (18)$$

where u_i s are arbitrary matrices, just replacing U^A by $U^{A,B}$. Because of the linearity of quantum operations, we can expect the validity of this proposition.

Ref. [11] generalized the HPV protocol to a protocol for the remote implementation of N -qubit operations that can be expressed as

$$U = \sum_{i=0}^{2^N-1} c_i |p_i(x), D\rangle\langle i, D|, \quad (19)$$

where D indicates the decimal system, i.e., $|0, D\rangle = |00\cdots 0\rangle$, $|1, D\rangle = |00\cdots 1\rangle$, $|2^N - 1, D\rangle = |11\cdots 1\rangle$, etc. And,

$$p(x) = \{p_0(x), p_1(x), \dots, p_{2^N-1}(x)\}, \quad (20)$$

is a certain permutation of the list $\{0, 1, \dots, 2^N - 1\}$, where $x = 1, 2, \dots, 2^N!$ labels all of the $2^N!$ permutations. We can similarly generalize the protocol in Sec. II.

Alice and Bob need locally implement an $(N + M)$ -qubit operation

$$U = \sum_{i=0}^{2^N-1} |p_i(x), D\rangle\langle i, D| \otimes u_i, \quad (21)$$

where u_i s are arbitrary $2^M \times 2^M$ unitary matrices. Bob has the device of U . Alice has the anterior N qubits named Y_1, Y_2, \dots, Y_N , and Bob has the posterior M qubits named Z_1, Z_2, \dots, Z_M . They share N maximally entangled pairs

$$|\Phi\rangle_{A_i B_i} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_i B_i}, \quad (i = 1, 2, \dots, N). \quad (22)$$

Alice has the qubits A_i s, and Bob has the qubits B_i s. The protocol can be expressed as the following steps.

step 1 Alice performs $CNOT^{Y_i, A_i}$ on every Y_i, A_i respectively. Then she measures every A_i in computational basis respectively and tell Bob the results.

step 2 If the measurement result of A_i is $|0\rangle$ Bob does nothing, if the result is $|1\rangle$ Bob performs X on B_i correspondingly.

step 3 Bob performs U on B_i s and Z_j s.

step 4 Bob performs an H on every B_i respectively. Then he measures every B_i in computational basis respectively and tell Alice the results.

step 5 Alice performs the permutation operation

$$R(x) = \sum_{i=0}^{2^N-1} |p_i(x), D\rangle\langle i, D|, \quad (23)$$

on Y_i s. Then if the measurement result of B_i is $|0\rangle$ Alice does nothing, if the result is $|1\rangle$ Alice performs Z on Y_i correspondingly.

After these 5 steps, Alice and Bob can locally implement the operation U on Y_1, Y_2, \dots, Y_N and Z_1, Z_2, \dots, Z_M using N ebits plus N cbits from Alice to Bob plus N cbits from Bob to Alice. Every $R(x)$ in step 5 can be implemented using two-qubit opearation CNOT and single-qubit operation X [11], so it is not too difficult to implement it.

The validity of this protocol can be proved using the methods similar to the appendix of Ref. [12]. The full proof can be found in Appendix A.

IV. MULTIPARTY

In the protocol in Sec. III, all of the operations performed by Alice are local to a certain qubit pair Y_i and A_i s, except for the permutation operation $R(x)$. So when $R(x)$ is a direct product of single-qubit operations (I or X), the protocol can be generalized to the multiparty cases — one node has the qubits B_i s and each of the other nodes has a pair of Y_i and A_i . We only discuss an example of three-party in this section. Other cases are all similar to it.

Consider a three-qubit diagonal block operation

$$U = \begin{pmatrix} u_{00} & & & \\ & u_{01} & & \\ & & u_{10} & \\ & & & u_{11} \end{pmatrix}, \quad (24)$$

where u_{ij} s are 2×2 unitary matrices. This operation is to be implemented on Alice, Bob, and Charlie's qubits A, B, C , and Charlie has the device. This operation can be expressed as

$$U^{A, B, C} = \sum_{i,j=0}^1 |i\rangle_A\langle i| \otimes |j\rangle_B\langle j| \otimes u_{ij}^C. \quad (25)$$

In general, this operation can not be transformed to the three-party control-U operation discussed in Ref. [1], but it can be locally implemented using the same method in Ref. [1].

Alice and Charlie share a maximally entangled pair $A_1 C_1$ as Eq. (4). Bob and Charlie share another maximally entangled pair $B_1 C_2$. They can use the protocol expressed in Fig. 3 to locally implement this operation.

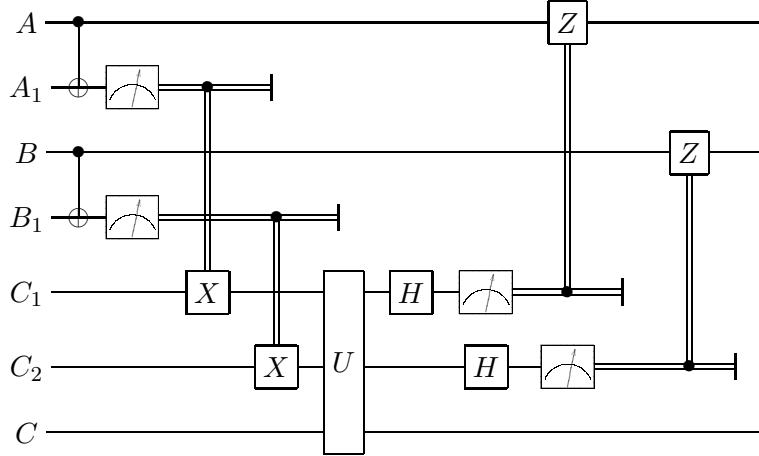


FIG. 3: Quantum circuit of the protocol for three-part diagonal block operation, A_1C_1 and B_1C_2 are maximally entangled pairs in the state defined by Eq. 4.

step 1 Alice performs a CNOT on her qubit A and A_1 . Then she measures A_1 in computational basis and tell the result to Charlie.

step 1' Bob performs a CNOT on her qubit B and B_1 . Then he measures B_1 in computational basis and tell the result to Charlie.

Obviously, step 1 and step 1' can be implemented in parallel.

step 2 If the measurement result of A_1 is $|1\rangle$ Charlie performs an X on C_1 , and if the result is $|0\rangle$ Charlie does nothing. If the measurement result of B_1 is $|1\rangle$ Charlie performs an X on C_2 , and if the result is $|0\rangle$ Charlie does nothing.

step 3 Charlie performs the three-qubit operation U on C_1, C_2, C .

step 4 Charlie performs an H on C_1 and C_2 respectively. Then he measures C_1 and C_2 in computational basis and tell the results to Alice and Bob respectively.

step 5 If the measurement result of C_1 is $|1\rangle$ Alice performs a Z on A , and if the result is $|0\rangle$ Alice does nothing.

step 5' If the measurement result of C_2 is $|1\rangle$ Bob performs a Z on B , and if the result is $|0\rangle$ Bob does nothing.

Thus, the three parters accomplish their task determinately using two ebits and four cbits. The validity of this protocol can be proved similarly.

V. CONCLUSION AND DISCUSSION

In this paper, we proved that any diagonal or offdiagonal block operations can be locally implemented using a similar protocol to the protocol for the CNOT operation, which is discussed in Ref. [1]. The protocol is independent on the dimension of the blocks. Then we compared the local implementation of nonlocal operations with the remote implementation of local operations, and pointed out a relation between them. Basing on this comparision, we generalized the protocols in Sec. II to the multiqubit cases in Sec. III. Finally, we generalized the protocol to the multiparty cases in Sec. IV.

Local implementations of nonlocal operations are important procedures in distributed quantum computation. These procedures can be implemented using entanglement resources and classical communications. Entanglement resources are precious in quantum information and quantum computation. So it is important to implement these procedures economically. The minimal resources of local implementation of some operations have been found, e.g., the CNOT operation. However, for most operations, the minimum is still unknown. Our method would provide some clues for this research.

Recent researches prefer to use Bell states as the entanglement resources. Nevertheless, other entanglement resources such as GHZ states are also important. So it is interesting to search appropriate protocols using these resources.

Acknowledgments

We acknowledge all the collaborators of our quantum theory group at the Institute for Theoretical Physics of our university. This work was funded by the National Natural Science Foundation of China under Grant No. 60573008.

APPENDIX A: PROOF OF OUR PROTOCOL

In this appendix, we prove the hybrid protocol proposed in Sec. III.

The initial state of the qubits $Y_1 Y_2 \cdots Y_N Z_1 Z_2 \cdots Z_M$ can always be expressed as

$$\begin{aligned}
& |\xi\rangle_{Y_1 Y_2 \cdots Y_N Z_1 Z_2 \cdots Z_M} \\
&= \sum_{k_1, k_2, \dots, k_{N+M}=0}^1 z_{k_1 k_2 \dots k_{N+M}} |k_1 k_2 \dots k_{N+M}\rangle \\
&= \sum_{k_1, k_2, \dots, k_N=0}^1 y_{k_1, k_2, \dots, k_N} |k_1, k_2, \dots, k_N\rangle_{Y_1 Y_2 \cdots Y_N} \otimes |\eta_{k_1, k_2, \dots, k_N}\rangle_{Z_1 Z_2 \cdots Z_M} \\
&= \sum_{m=0}^{2^N-1} y_m |m, D\rangle_{Y_1 Y_2 \cdots Y_N} \otimes |\eta_m\rangle_{Z_1 Z_2 \cdots Z_M},
\end{aligned} \tag{A1}$$

where $|\eta_{k_1, k_2, \dots, k_N}\rangle$ s or $|\eta_m\rangle$ s need not be orthogonal each other. So the initial state of the total system can be expressed as

$$\begin{aligned}
& |\Psi^{\text{ini}}\rangle \\
&= \left(\bigotimes_{m=1}^N |\Phi\rangle_{A_m B_m} \right) \otimes |\xi\rangle_{Y_1 Y_2 \cdots Y_N Z_1 Z_2 \cdots Z_M} \\
&= \frac{1}{\sqrt{2^N}} \sum_{k_1, k_2, \dots, k_N=0}^1 y_{k_1, k_2, \dots, k_N} \bigotimes_{i=1}^N \left[\left(\sum_{j=0}^1 |jj\rangle_{A_i B_i} \right) |k_i\rangle_{Y_i} \right] \otimes |\eta_{k_1, k_2, \dots, k_N}\rangle_{Z_1 Z_2 \cdots Z_M}.
\end{aligned} \tag{A2}$$

After step 1, the state becomes

$$\begin{aligned}
|\Psi^1\rangle &= \frac{1}{\sqrt{2^N}} \sum_{k_1, k_2, \dots, k_N=0}^1 y_{k_1, k_2, \dots, k_N} \\
&\quad \left\{ \bigotimes_{i=1}^N \left[(|a_i\rangle_{A_i} \langle a_i|) CNOT^{Y_i, A_i} \right] \sum_{j=0}^1 |jj\rangle_{A_i B_i} |k_i\rangle_{Y_i} \right\} \otimes |\eta_{k_1, k_2, \dots, k_N}\rangle_{Z_1 Z_2 \cdots Z_M} \\
&= \frac{1}{\sqrt{2^N}} \sum_{k_1, k_2, \dots, k_N=0}^1 y_{k_1, k_2, \dots, k_N} \left\{ \bigotimes_{i=1}^N |a_i\rangle_{A_i} |k_i \oplus a_i\rangle_{B_i} |k_i\rangle_{Y_i} \right\} \otimes |\eta_{k_1, k_2, \dots, k_N}\rangle_{Z_1 Z_2 \cdots Z_M}
\end{aligned} \tag{A3}$$

where $|a_i\rangle$ s is the measurement results of A_i s. Every item in the bracket $\{\}$ is calculated similar to Sec. II.

After step 2, the state of $Y_1 Y_2 \cdots Y_N Z_1 Z_2 \cdots Z_M B_1 B_2 \cdots B_N$ becomes

$$\begin{aligned}
& \sum_{k_1, k_2, \dots, k_N=0}^1 y_{k_1, k_2, \dots, k_N} \left\{ \bigotimes_{i=1}^N |k_i\rangle_{B_i} |k_i\rangle_{Y_i} \right\} \otimes |\eta_{k_1, k_2, \dots, k_N}\rangle_{Z_1 Z_2 \cdots Z_M} \\
&= \sum_{m=0}^{2^N-1} y_m |m, D\rangle_{B_1 B_2 \cdots B_N} |m, D\rangle_{Y_1 Y_2 \cdots Y_N} \otimes |\eta_m\rangle_{Z_1 Z_2 \cdots Z_M}.
\end{aligned} \tag{A4}$$

Every item in the bracket $\{\}$ is gotten similar to Sec. II.

After step 3, the state of $Y_1 Y_2 \cdots Y_N Z_1 Z_2 \cdots Z_M B_1 B_2 \cdots B_N$ becomes

$$\begin{aligned} |\Psi^3\rangle &= U^{B_1 B_2 \cdots B_N Z_1 Z_2 \cdots Z_M} \sum_{m=0}^{2^N-1} y_m |m, D\rangle_{B_1 B_2 \cdots B_N} |m, D\rangle_{Y_1 Y_2 \cdots Y_N} \otimes |\eta_m\rangle_{Z_1 Z_2 \cdots Z_M} \\ &= \sum_{m=0}^{2^N-1} y_m |p_m(x), D\rangle_{B_1 B_2 \cdots B_N} |m, D\rangle_{Y_1 Y_2 \cdots Y_N} \otimes (u_m |\eta_m\rangle)_{Z_1 Z_2 \cdots Z_M}. \end{aligned} \quad (\text{A5})$$

Denote

$$|p_m(x), D\rangle_{B_1 \cdots B_N} = \bigotimes_{i=1}^N |l_m^i(x)\rangle_{B_i}, \quad (l_m^i(x) = 0, 1). \quad (\text{A6})$$

Then,

$$|\Psi^3\rangle = \sum_{m=0}^{2^N-1} y_m |m, D\rangle_{Y_1 \cdots Y_N} \otimes (u_m |\eta_m\rangle)_{Z_1 Z_2 \cdots Z_M} \otimes \bigotimes_{i=1}^N |l_m^i(x)\rangle_{B_i}. \quad (\text{A7})$$

So, after step 4 the state of $Y_1 Y_2 \cdots Y_N Z_1 Z_2 \cdots Z_M$ becomes

$$\sum_{m=0}^{2^N-1} y_m (-1)^{\sum_{i=1}^N l_m^i(x) b_i} |m, D\rangle_{Y_1 \cdots Y_N} \otimes (u_m |\eta_m\rangle)_{Z_1 Z_2 \cdots Z_M}, \quad (\text{A8})$$

Where b_i s are the measurement results of B_i s. The coefficient $(-1)^{\sum_{i=1}^N l_m^i(x) b_i}$ is gotten similar to Sec. II. Apparently,

$$R(x) |m, D\rangle = |p_m(x), D\rangle = \bigotimes_{i=1}^N |l_m^i(x)\rangle. \quad (\text{A9})$$

So after step 5 the state of $Y_1 Y_2 \cdots Y_N Z_1 Z_2 \cdots Z_M$ becomes

$$\begin{aligned} &\sum_{m=0}^{2^N-1} y_m (-1)^{\sum_{i=1}^N l_m^i(x) b_i} \bigotimes_{i=1}^N [(Z^{b_i}) |l_m^i(x)\rangle]_{Y_i} \otimes (u_m |\eta_m\rangle)_{Z_1 Z_2 \cdots Z_M} \\ &= \sum_{m=0}^{2^N-1} y_m (-1)^{\sum_{i=1}^N l_m^i(x) b_i} \bigotimes_{i=1}^N (-1)^{l_m^i(x) b_i} |l_m^i(x)\rangle_{Y_i} \otimes (u_m |\eta_m\rangle)_{Z_1 Z_2 \cdots Z_M} \\ &= \sum_{m=0}^{2^N-1} y_m \bigotimes_{i=1}^N |l_m^i(x)\rangle_{Y_i} \otimes (u_m |\eta_m\rangle)_{Z_1 Z_2 \cdots Z_M} \\ &= \sum_{m=0}^{2^N-1} y_m |p_m(x), D\rangle_{Y_1 Y_2 \cdots Y_N} \otimes (u_m |\eta_m\rangle)_{Z_1 Z_2 \cdots Z_M} \\ &= U |\xi\rangle_{Y_1 Y_2 \cdots Y_N Z_1 Z_2 \cdots Z_M} \end{aligned} \quad (\text{A10})$$

Thus, we accomplish the proof.

- [1] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000)
- [2] S. F. Huelga, J. A. Vaccaro, A.Chefles, and M. B. Plenio, Phys. Rev. A **63**, 042303 (2001)
- [3] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993)
- [4] D. Collins, N. Linden, and S. Popescu, Phys. Rev. A **64**, 032302 (2001).
- [5] Y.-F Huang, X.-F Ren, Y.-S. Zhang, L.-M. Duan, and G.-C Guo, Phys. Rev. Lett. **93**, 240501 (2004)
- [6] W. Dür and J. I. Cirac, Phys. Rev. A **64**, 012317 (2001).
- [7] W. Dür, G. Vidal, J. I. Cirac, N. Linden, and S. Popescu, Phys. Rev. Lett. **87**, 137901 (2001).

- [8] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. Lett. **89**, 057901 (2002)
- [9] Yong-Sheng Zhang, Ming-Yong Ye, and Guang-Can Guo, Phys. Rev. A **71**, 062331 (2005)
- [10] S. F. Huelga, M. B. Plenio, and J. A. Vaccaro, Phys. Rev. A **65**, 042316 (2002)
- [11] A. M. Wang, Phys. Rev. A **74**, 032317 (2006)
- [12] N. B. Zhao, A. M. Wang, Phys. Rev. A **76**, 062317 (2007)